State of South Dakota

Bureau of Information & Telecommunications

Monthly Cyber Security Newsletter

February 2014 | Volume 9, Issue 2

Personal Backup and Recovery of Your Data

What Are Backups?

Backups of computers, laptops and other devices are important defense layers in recovering from intentional or unintentional loss or corruption of data. For example, critical information can be lost when your hard drive becomes corrupted; natural disasters can destroy your equipment and device; or malware could infect your computer or device and corrupt your data. With a solid backup and recovery plan, you have a greater chance of recovering from any of these scenarios; without one, those chances are significantly diminished.

There are many different options for backing up and storing your information, and listed below are the commonly used methods.

Types of Backups

- **Full backup:** A full backup includes all files and software. It is important to consider the amount of storage necessary, and the amount of time it would take to not only back up all this information, but also to recover.

- **Incremental backup:** In this strategy, a full backup would need to be done periodically, and then only files that have been changed since the last full backup will be replicated. As an example, a full backup may be performed monthly and a differential backup (only the changed information) everyday at 5pm. Differential backups are beneficial in this case because they take less time to conduct, and recovery of information can be more exact to the time the information was compromised or lost.

Backup Storage Options

- **External Drive:** One of the more common methods of backing up information is storing the backup image on a portable drive. This way, if the hard drive on your computer fails, your backup files are still available to restore. To implement this solution an additional device must be purchased and connected to your computer. If the external device is disconnected, your backup will not be performed as scheduled.

- **Cloud-Based Backup:** Performing backups to the cloud is becoming more common. Usually this is done via a paid cloud service. Things to consider include cost and location of storage as well as the security controls that the cloud provider has in place. Additionally, be aware that with cloud solutions, backups and recovery speeds are dependent on the speed of your Internet connection.

- **Hard Drive**
  Another common method of backing up information requires the use of an allocated area of the hard drive of your computer. While the process is simple to implement and adds no additional costs, the risk associated with this method is the potential loss of all your information and also all your backed up information should you have a serious hard drive failure.

Developing a Backup Plan

Consider the following when developing a plan:

- **How important is the information on your systems or devices?** For critical information, such as contact lists, email, financial transactions, or related business files, you may want to have redundant backup. For less important information, you could back up the information with less frequency.
- **How often does the information change?** The frequency of change can affect your decision on how often the information should be backed up. For example, critical information that changes daily should be backed up daily.
- **How quickly do you need to recover the information?** Time is an important factor in creating a backup plan. For critical information, such as business files, you may need to recover your information quickly.
- **Do you have the resources to perform backups?** You must have backup hardware of sufficient capacity and software to perform backups.
- **What is the best time to schedule backups?** Scheduling backups when system use is as low as possible (such as overnight) will speed the backup process.

Recovery

Backing up data is futile if you cannot recover it. While automated backup strategies are usually efficient, it is a good idea to check on your backup data periodically. This is important not only to make sure the data is actually backed up and also to review the backup settings.

For More Information

Center for Internet Security: Cyber Security Guides
http://msisac.cisecurity.org/resources/guides/
SANS Securing the Human: Personal Backup and Recovery
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_en.pdf
EDGIS Security: SANS OUCH! – Personal Backup and Recovery
http://edgis-security.org/awareness-2/sans-ouch-personal-backup-and-recovery/

Brought to you by: